
CONTENTS

APPROVAL	ii
SELF DECLARATION AGAINST PLAGIARISM	iii
ABSTRACT	iv
ABSTRAK	v
DEDICATION	vi
ACKNOWLEDGMENTS	vii
PREFACE	viii
CONTENTS	ix
LIST OF TABLES	xii
LIST OF FIGURES	xiii
1 INTRODUCTION	1
1.1 Rationale	1
1.2 Theoretical Framework.....	1
1.3 Conceptual Framework/Paradigm.....	2
1.4 Statement of the Problem	2
1.5 Objective and Hypotheses.....	3
1.6 Assumption	3
1.7 Scope and Delimitation	3
1.8 Significance of the Study.....	3
2 REVIEW OF LITERATURE AND STUDIES	5
2.1 Related Literatures	5
2.1.1 Zero-knowledge concept.....	5
2.1.2 Deniable Authentication.....	7
2.1.3 Keccak hash function.....	7
2.1.4 Impersonation Attack	10
2.1.5 Man-In-The-Middle attack (MITM)	11
2.2 Li-Takagi's Scheme and Its Security Analysis	12
2.2.1 Li-Takagi's Scheme	12
2.2.2 Security Analysis of Li-Takagi's Scheme	15

3 RESEARCH METHODOLOGY	19
3.1 Overview of the Proposed Scheme	19
3.1.1 The Difference between the Previous and the Proposed Scheme.....	21
3.1.2 The Proposed Scheme using Zero Knowledge Concepts.....	21
3.2 Evaluation Scenario	29
3.3 Analysis	29
3.3.1 Performance of scheme	29
3.3.2 Probability of success attack.....	29
3.3.3 Provable security of the scheme.....	30
4 PRESENTATION, ANALYSIS AND INTERPRETATION OF DATA	31
4.1 Presentation of Data	31
4.1.1 Li-Takagi's Performance	31
4.1.2 Proposed Scheme Performance	32
4.2 Attacks on the Proposed Scheme	33
4.2.1 Impersonation Attack of the Proposed Scheme	33
4.2.2 Man-In-The-Middle attack (MITM) Attack on the Propsed Scheme .	34
4.2.3 Provable Security.....	36
4.3 Summary of Findings.....	42
5 CONCLUSION AND RECOMMENDATIONS	44
5.1 Conclusions	44
5.2 Recommendations.....	44
BIBLIOGRAPHY	45
Appendices	46
A The algorithm and Complexity of The Large Integer Exponentiation in the Modulus	48
B The algorithm and Complexity of The Keccak Hash Function	49
C The algorithm and Complexity of Attacks on Li-Takagi and The Proposed scheme	53
D The encryption process in the receiver using the sender's public key	55
E The decryption process in the sender using the sender's secret key	58
F The xor-ed process of c2 and c1 or M and c1	61
G The encryption process in the sender using the receiver's public key	63

H The decryption process in the receiver using the receiver's secret key	65
---	-----------

I Curriculum Vitae # Example	68
-------------------------------------	-----------